EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	9	("6026163").URPN.	USPAT	OR	ON	2007/03/02 14:02
L3	3	("5625692" | "6026163" | "6237097").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/03/02 14:54
L4	0	("7187771").PN.	US-PGPUB; USPAT	OR	OFF	2007/03/02 14:54
L5	15	("20020004783" | "5191193" | "5878138" | "5937066" | "5970475" | "5982293" | "6118874" | "6220510" | "6263313" | "6282653" | "6317832" | "6328217" | "6357665" | "6567915" | "6738899").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/03/02 15:46
S1	1	("20040103292").PN.	US-PGPUB; USPAT	OR	OFF	2007/03/01 15:24
S2	248	(380/286).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/03/02 11:37
S3	244	(380/283).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/03/02 11:37
S4	133	(split$4 divid$3 subdivid$3 apportion$3) adj (key) same (scrambl$3 encrypt$3 encipher$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/02 11:39

Other search results was not saved.

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+encryption "split key" "split-key" SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **encryption split key split key**

Found **145** of **8 searched out of 198,146.**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 145

Result page: **1** 2 3 4 5 6 7 8 next

Relevance scale

1 A taxonomy for key escrow encryption systems

Dorothy E. Denning, Dennis K. Branstad

March 1996 **Communications of the ACM,** Volume 39 Issue 3

Publisher: ACM Press

Full text available: pdf(548.67 KB) Additional Information: full citation, citings, index terms, review

2 Communications privacy: implications for network design

Marc Rotenberg

August 1993 **Communications of the ACM,** Volume 36 Issue 8

Publisher: ACM Press

Full text available: pdf(2.91 MB) Additional Information: full citation, references, index terms, review

3 Inside risks: risks of insiders

Peter G. Neumann

December 1999 **Communications of the ACM,** Volume 42 Issue 12

Publisher: ACM Press

Full text available: pdf(45.43 KB) html(7.68 KB) Additional Information: full citation, citings, index terms

4 Wireless sensor networks: An efficient key establishment scheme for secure aggregating sensor networks

Erik-Oliver Blaß, Martina Zitterbart

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available: pdf(252.38 KB) Additional Information: full citation, abstract, references, index terms

Key establishment is a fundamental prerequisite for secure communication in wireless sensor networks. A new node joining the network needs to efficiently and autonomously set up secret keys with his communication partners without the use of a central infrastructure. Most cited current research papers focus on a probabilistic distribution of sets of keys from larger *key pools* to new nodes. This results in unnecessary expensive communication and memory consumption, growing linearly with the ...

Keywords: aggregation, efficiency, key establishment, sensor networks

5 Verifiable partial key escrow
Mihir Bellare, Shafi Goldwasser
April 1997 **Proceedings of the 4th ACM conference on Computer and communications security CCS '97**
Publisher: ACM Press
Full text available: pdf(1.98 MB) Additional Information: full citation, references, citings, index terms

6 Cryptographic key management
Dahl A. Gerberick
May 1990 **ACM SIGSAC Review**, Volume 8 Issue 2
Publisher: ACM Press
Full text available: pdf(962.96 KB) Additional Information: full citation, abstract, index terms

There are two main issues concerning data security on networks; controlling access and the vulnerability of data communication links. A brief introduction to the various techniques which may be applied to these concerns are given in this paper.

7 Commentators
Mike Godwin, William A. Bayse, Marc Rotenberg, Lewis M. Branscomb, Anne M. Branscomb, Ronald L. Rivest, Andrew Grosso, Gary T. Marx
March 1993 **Communications of the ACM**, Volume 36 Issue 3
Publisher: ACM Press
Full text available: pdf(6.12 MB) Additional Information: full citation, references, index terms

8 Multi party computations: past and present
Shafi Goldwasser
August 1997 **Proceedings of the sixteenth annual ACM symposium on Principles of distributed computing PODC '97**
Publisher: ACM Press
Full text available: pdf(439.35 KB) Additional Information: full citation, references, citings, index terms

9 Applied cryptography II: Stateful public-key cryptosystems: how to encrypt with one 160-bit exponentiation
Mihir Bellare, Tadayoshi Kohno, Victor Shoup
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(235.26 KB) Additional Information: full citation, abstract, references, index terms

We show how to significantly speed-up the encryption portion of some public-key cryptosystems by the simple expedient of allowing a sender to maintain state that is re-used across different encryptions.In particular we present stateful versions of the DHIES and Kurosawa-Desmedt schemes that each use only 1 exponentiation to encrypt, as opposed to 2 and 3 respectively in the original schemes, yielding the fastest discrete-log based public-key encryption schemes known in the random-oracle and stan ...

Keywords: cryptography, public-key encryption

10 Data protection: Attribute-based encryption for fine-grained access control of encrypted data □

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**

Publisher: ACM Press

Full text available: pdf(277.46 KB) Additional Information: full citation, abstract, references, index terms

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and pri ...

Keywords: access control, attribute-based encryption, audit logs, broadcast encryption, delegation, hierarchical identity-based encryption

11 Data protection: Searchable symmetric encryption: improved definitions and efficient constructions □

Reza Curtmola, Juan Garay, Seny Kamara, Rafail Ostrovsky

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**

Publisher: ACM Press

Full text available: pdf(682.40 KB) Additional Information: full citation, abstract, references, index terms

Searchable symmetric encryption (SSE) allows a party to outsource the storage of its data to another party (a server) in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research in recent years. In this paper we show two solutions to SSE that simultaneously enjoy the following properties:

1. Both solutions are more efficient than all previous constant-round schemes. In particular, the work performed by the server per r ...

   Keywords: multi-user, searchable encryption, searchable symmetric encryption, security definitions

12 Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm □

Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre

May 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 2

Publisher: ACM Press

Full text available: pdf(404.99 KB) Additional Information: full citation, abstract, references, index terms, review

The *secure shell* (SSH) protocol is one of the most popular cryptographic protocols on the Internet. Unfortunately, the current SSH authenticated encryption mechanism is insecure. In this paper, we propose several fixes to the SSH protocol and, using techniques from modern cryptography, we prove that our modified versions of SSH meet strong new chosen-ciphertext privacy and integrity requirements. Furthermore, our proposed fixes will require relatively little modification to the SSH protoc ...

Keywords: Authenticated encryption, secure shell, security proofs, stateful decryption

13 Verifiable encryption of digital signatures and applications □
Giuseppe Ateniese
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press
Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fair exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

14 Image processing: The encryption method to share a secret binary image and its decryption system □
Sang-su Lee, Jong-wook Han, Hyo-wook Bae
September 2003 **Proceedings of the 1st international symposium on Information and communication technologies ISICT '03**
Publisher: Trinity College Dublin
Full text available: pdf(156.34 KB) Additional Information: full citation, abstract, references

In this paper, an encryption method to share a secret binary image was proposed. This divides the image to be encrypted into an arbitrary number of images and encrypts them using XOR process with different binary random images which was prepared by the means of the XOR process, too. Each encrypted slice image can be distributed to the authenticated ones. However, we transfer the encrypted images to the binary phase masks to strengthen the security power, that means phase masks can not be copied ...

Keywords: cryptography, data security, image reconstruction, optical imaging

15 Efficient Memory Integrity Verification and Encryption for Secure Processors □
G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas
December 2003 **Proceedings of the 36th annual IEEE/ACM International Symposium on Microarchitecture MICRO 36**
Publisher: IEEE Computer Society
Full text available: pdf(307.01 KB) Additional Information: full citation, abstract, citings, index terms

Secure processors enable new sets of applications suchas commercial grid computing, software copy-protection,and secure mobile agents by providing security from bothphysical and software attacks. This paper proposes newhardware mechanisms for memory integrity verification andencryption, which are two key primitives required in single-chipsecure processors. The integrity verification mechanismoffers significant performance advantages over existingones when the checks are infrequent as in grid com ...

16 Embedded applications: Encryption overhead in embedded systems and sensor network nodes: modeling and analysis □
Ramnath Venugopalan, Prasanth Ganesan, Pushkin Peddabachagari, Alexander Dean, Frank

Mueller, Mihail Sichitiu
October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems CASES '03**
Publisher: ACM Press
Full text available: pdf(293.59 KB) Additional Information: full citation, abstract, references, citings, index terms

Recent research in sensor networks has raised issues of security for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combi ...

Keywords: embedded systems, encryption, security, sensor networks

17 Supporting cryptographic technology: Broadcast encryption with short keys and transmissions □
Nuttapong Attrapadung, Kazukuni Kobara
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(269.23 KB) Additional Information: full citation, abstract, references, citings, index terms

Broadcast Encryption allows a broadcaster to broadcast an encrypted message so that only a dynamically changing designated group of users can decrypt it. The stateless setting considers the case where the private key at each user is never updated. A central open problem in this area is to design a stateless scheme where both the size of transmission header which encapsulates the session key and the size of private key at each user are small and *independent* of the number of users (all/priv ...

Keywords: broadcast encryption, constant transmission rate, copyright protection, one-way accumulators, revocation scheme

18 Security: Analyzing and modeling encryption overhead for sensor network nodes □
Prasanth Ganesan, Ramnath Venugopalan, Pushkin Peddabachagari, Alexander Dean, Frank Mueller, Mihail Sichitiu
September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications WSNA '03**
Publisher: ACM Press
Full text available: pdf(254.57 KB) Additional Information: full citation, abstract, references, citings, index terms

Recent research in sensor networks has raised security issues for small embedded devices. Security concerns are motivated by the deployment of a large number of sensory devices in the field. Limitations in processing power, battery life, communication bandwidth and memory constrain the applicability of existing cryptography standards for small embedded devices. A mismatch between wide arithmetic for security (32 bit word operations) and embedded data bus widths (often only 8 or 16 bits) combined ...

Keywords: analysis, embedded systems, encryption overhead, model, sensor networks

19 OCB: A block-cipher mode of operation for efficient authenticated encryption □
Phillip Rogaway, Mihir Bellare, John Black

August 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 3
Publisher: ACM Press
Full text available: pdf(568.74 KB) Additional Information: full citation, abstract, references, index terms

We describe a parallelizable block-cipher mode of operation that simultaneously provides privacy and authenticity. OCB encrypts-and-authenticates a nonempty string *M* &in; &lcub;0, 1&rcub;* using □&vertbar;*M*&vertbar;/*n*□ + 2 block-cipher invocations, where *n* is the block length of the underlying block cipher. Additional overhead is small. OCB refines a scheme, IAPM, suggested by Charanjit Jutla. Desirable properties of OCB include the ability to encrypt a bi ...

Keywords: AES, authenticity, block-cipher usage, cryptography, encryption, integrity, modes of operation, provable security, standards

20 Implementing encrypted home directories □
Mike Petullo
August 2003 **Linux Journal**, Volume 2003 Issue 112
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(19.37 KB) Additional Information: full citation, abstract

Keep your files safely encrypted when you're logged out, and automatically get access when you log in.

Results 1 - 20 of 145 Result page: **1** 2 3 4 5 6 7 8 next

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player